COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

JOHN NAIMO
AUDITOR-CONTROLLER

February 8, 2016

TO: Robin Kay, Ph.D., Acting Director
Department of Mental Health

FROM: John Naimo
Auditor-Controller

SUBJECT: **HIPAA AND HITECH ACT COMPLIANCE REVIEW – ANTELOPE VALLEY MENTAL HEALTH CENTER AND WELLNESS CENTER**

We have completed a review of the Department of Mental Health (DMH) Antelope Valley Mental Health Center's (AVMHC) and Wellness Center's compliance with the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic Clinical Health (HITECH) Act.[1] On December 2, 2015, we provided your Department with our final draft report, and conducted an exit conference on December 7, 2015. This report includes our findings, recommendations for corrective action, and your Department's response.

Approach/Scope

Our review utilized the *HIPAA Privacy Rule and Health Information Technology for Economic Clinical Health (HITECH) Act Audit Tool* in evaluating AVMHC's and Wellness Center's compliance with the HIPAA Privacy Rule and DMH's HIPAA policies and procedures. DMH management is responsible for establishing and maintaining effective internal compliance with HIPAA regulations, and has oversight of the HIPAA program throughout their facilities. We considered DMH's internal controls over their compliance program, and the HIPAA Privacy Rule requirements that could have a direct and material effect on AVMHC.

Our review covered the HIPAA Privacy Rule requirements for:

- Notice of Privacy Practices (NPP) for protected health information (PHI)
- Safeguards for PHI

[1] 45 Code of Federal Regulations Parts 160 and 164

- Training
- Complaint process
- Refraining from intimidating or retaliatory acts
- Uses and disclosures requiring authorization
- Accounting for disclosures of PHI
- Minimum necessary standard
- HITECH Act Breach Notification Rule

Results of Review and Recommendations

Notice of Privacy Practices for Protected Health Information

The HIPAA Privacy Rule requires a covered entity with direct treatment relationships with individuals to give the NPP to every individual no later than the date of first service delivery, and to make a good faith effort to obtain the individual's written acknowledgment of receipt of the NPP. If the provider maintains an office or other physical site where care is provided directly to individuals, the provider must also post the NPP in the facility in a clear and prominent location where individuals are likely to see it, as well as make the NPP available to those who ask for a copy.[2]

During our on-site review of AVMHC's main clinic and Wellness Center (which is a satellite program located at a separate location), we observed that the updated DMH NPP was displayed in a prominent location. In addition, we confirmed that the NPP is available on DMH's Internet web site for patients to access without having to make a request.

We randomly selected ten (closed and active) medical charts to verify the AVMHC management's statement that all patients are given the NPP on their first service delivery date, and noted that all the charts included the patient's signed acknowledgment of receipt form.

Based on these findings, it appears that AVMHC is in compliance with the NPP for PHI standard.

Safeguards for Protected Health Information

A covered entity must have in place appropriate administrative, physical, and technical safeguards to protect the privacy of PHI. A covered entity must reasonably safeguard PHI and electronic PHI, and make reasonable efforts to prevent any intentional or unintentional use or disclosures that violate the HIPAA Privacy Rule.

---

[2] Ibid., §164.520(c)

Technical Safeguards

DMH's Chief Information Office Bureau (CIOB) informed us that DMH is fully compliant with the Board's May 27, 2014 motion, which requires all County workstation hard drives to be encrypted to protect personally identifiable information and PHI. CIOB also informed us that all DMH workstations and laptop computers are equipped and protected with anti-malware/anti-virus software and port control software, which block downloading of PHI or other data to portable storage devices; and, the computers are configured to prevent workforce members from saving PHI onto their hard drives.

To evaluate whether individual workstations at AVMHC were equipped with encryption software, we obtained a report from DMH Information Technology (IT) staff of all workstations at AVMHC that were connected to DMH servers, and compared that list with a data encryption report generated by DMH's encryption software, WinMagic SecureDoc Enterprise Server. The report identified 42 connected workstations at AVMHC, and all of them were reported to be encrypted. We did not inspect workstations or separately verify the encryption status of individual computers.

Access Controls

CIOB also represented that they are responsible for removing employee access to IT resources, including systems which contain electronic PHI, when they receive notification from DMH's Human Resources Bureau (HRB) that an employee has terminated service or transferred to another County department. In addition, CIOB indicated that an automated process disables accounts that are inactive for 90 days, and terminates accounts 60 days after they are disabled. As a result, unused accounts are automatically disabled to prevent inappropriate access to resources in the event HRB fails to provide notification to CIOB. We noted that these automated controls would not detect or prevent staff from misusing a former employee's credentials to access IT resources.

We reviewed documentation provided by CIOB to remove IT system access for AVMHC employees who terminated service between 2012 and 2015, and noted that three (27%) of the 11 former employees' accounts were not terminated timely (i.e., CIOB indicated they did not receive notification from HRB of the terminations). The three accounts were ultimately terminated due to non-activity via the automated process described above, and we found no evidence that these accounts were accessed after the employees terminated service. Nevertheless, these findings indicate that HRB and CIOB staff may not always be communicating effectively regarding changes in employee status.

We also reviewed DMH Policy Number 560.01, *County Property and Systems Access Clearance for Terminations and Interdepartmental Transfers,* and DMH's Terminating Resource Access to DMH Users Procedures. While these procedures describe how

HRB should communicate terminations/transfers to CIOB, they do not address monitoring (e.g., periodically comparing lists of terminated employees to lists of active IT system users) to ensure that all terminated employees' access is removed timely.

Recommendation

1. **Department of Mental Health management establish and/or strengthen procedures to ensure that user accounts and access to information technology resources for transferred and/or terminated employees and contractors are disabled/removed timely. Procedures should clearly describe the process for communicating terminations and transfers to security administrators, and for monitoring, reviewing, and terminating access, as appropriate.**

Administrative and Physical Safeguards

During our on-site review of the main clinic and Wellness Center, we verified that the fax machine, copier, and network printer were maintained in secure areas, and no PHI was left unattended on or near the equipment during our review. In addition, we reviewed whether proper safeguards were implemented in areas where medical records are stored at both the main clinic and Wellness Center. Our findings for each of the areas we reviewed are detailed below.

Main Clinic

We observed and were informed by AVMHC management that the main clinic's medical charts are stored in rolling lockable cabinets in a designated storage room, which is secured with a key lock, and accessible only by the assigned medical records staff and AVMHC management. In addition, AVMHC transitioned to electronic medical records in August 2014 with the implementation of the Integrated Behavioral Health Information System (IBHIS), and we were told that AVMHC workforce members now rarely access the paper charts.[3] We observed that the medical records storage room was locked during our visit. Discussions with the medical records staff and a review of a sample of chart tracking log indicate that the main clinic has adequate procedures in place for the management of their medical records.

Wellness Center

AVMHC management stated, and we observed, that the Wellness Center's medical charts are kept in lockable cabinets in a designated storage room, which is secured with a keypad lock and accessible by all staff at the Wellness Center. AVMHC management

[3] The IBHIS provides DMH clinicians access to client clinical records regardless of where each client was seen previously in the DMH network. Clinicians will have access to medication history information, recent assessments, laboratory and psychological test results, and, when appropriate, clinician notes from prior visits.

indicated that most charts have been converted to IBHIS, and the paper charts are rarely used. Clinicians use a manual, self-reported log to track the paper charts. We informed AVMHC management that their access procedures do not adequately safeguard PHI, and recommended that AVMHC promptly implement stronger controls over medical charts.

During our on-site review of the Wellness Center, we observed some documents containing PHI that were left unsecured in the cubicle of an employee who often works in the field, and was away during our visit. Because the workstation is in an area frequented by clients, we asked AVMHC management to remind all employees to ensure that they safeguard PHI to prevent incidental or prohibited disclosures.

Based on these findings, it appears that AVMHC failed to implement reasonable administrative and physical safeguards to fully safeguard PHI from wrongful disclosure.

Recommendations

Antelope Valley Mental Health Center management:

2. **Ensure that the Wellness Center's medical records storage room is properly secured by restricting access to only those workforce members who have a business need, and assign a workforce member to log and track the removal and return of paper charts.**

3. **Remind Wellness Center workforce members to take precautions to prevent unauthorized physical access to sensitive information, including storing protected health information in locked drawers or cabinets when unattended.**

Training

As a HIPAA covered program, AVMHC must train all workforce members on policies and procedures related to PHI as required by the HIPAA Privacy and Security Rules, and retrain staff when regulations are updated, to the extent necessary and appropriate for their jobs. Workforce members include employees, volunteers, and trainees.

The DMH Privacy Officer stated that HRB is responsible for ensuring its workforce members are trained on HIPAA compliance via the County's Learning Net system. AVMHC management is responsible for training new-hires on DMH's HIPAA policies and procedures, and for any additional role-based training for individual workforce members. In addition, as part of the annual performance evaluation process, management reviews relevant DMH policies, including on HIPAA, with the employee being rated; and, the manager and employee sign an acknowledgment documenting the review.

Our review of the AVMHC's HIPAA training records showed that 11 (two on long-term leave, three new-hires within 60 days of employment, one volunteer, and five locum or contracted individuals) out of 33 (33%) workforce members had not completed the required HIPAA training. AVMHC management stated that the locum workforce members were provided with basic HIPAA information, but we could not find any evidence that they met the training requirement.

It appears that AVMHC is not in compliance with the training standard.

Recommendation

4. **Antelope Valley Mental Health Center management ensure all workforce members, including locum employees, promptly receive the required HIPAA training, and maintain evidence documenting that training was completed.**

Complaint Process

A covered entity must provide a process for patients to complain about its policies and procedures. In addition, a covered entity must document all complaints received and their disposition, if any.

AVMHC management informed us that patient complaints are handled in accordance with DMH Policy Number 500.11, *HIPAA Privacy Complaints*, and AVMHC's internal protocols. Patients are directed to contact the Program Head or DMH's Patients' Rights Office to file a complaint.

We observed that the DMH NPP posted in the waiting area appropriately informs patients that they may file a complaint with the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR), the County's Chief HIPAA Privacy Officer (CHPO), and/or DMH's Patients' Rights Office. We randomly selected three workforce members who were on-site at the time of our visit and interviewed them to test their knowledge about assisting patients who may wish to file a complaint. Their responses indicated that they are familiar with the complaint procedure and had received appropriate training in this area. In the past year, no complaints were filed with the CHPO by AVMHC patients. It appears that the AVMHC complaint process complies with the complaints process standard.

Refraining from Intimidating or Retaliatory Acts

Discussions with AVMHC management confirm they are aware of their obligation to comply with DMH Policy Number 500.18, *Refraining from Retaliatory or Intimidating Acts Against Individuals That Assert Rights Under HIPAA*. They also understand that OCR will investigate complaints against a covered entity that asserts retaliatory actions.

In the past year, no complaints related to retaliatory or intimidating acts were filed with the CHPO by AVMHC patients. It appears that AVMHC is in compliance with the refraining from intimidating or retaliatory acts standard.

Uses and Disclosures Requiring Authorization

OCR defines an authorization as a detailed document that gives covered entities permission to use PHI for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose PHI to a third party specified by the patient. An authorization must specify a number of elements, including: (1) a description of the PHI to be used and disclosed, (2) the person authorized to make the use or disclosure, (3) the person to whom the covered entity may make the disclosure, (4) an expiration date, and (5) the purpose for which the information may be used or disclosed.

AVMHC management reported that they follow DMH Policy Number 500.1, *Use and Disclosure of Protected Health Information Requiring Authorization.* Our review of the policy and the authorization form noted that they meet the Uses and Disclosures Requiring Authorization standard. During our on-site review, we reviewed seven completed authorization forms, which were found in the above-mentioned ten medical charts, and noted that the majority of the forms were properly filled out, with two exceptions. We found that one form did not include the purpose for the disclosure and the other form did not include the date of the request. We asked AVMHC management to remind workforce members to ensure that all required fields in the authorization form are completed when working with clients. Overall, we found that AVMHC workforce members are generally adhering to the uses and disclosures requiring authorization standard.

Accounting for Disclosures of Protected Health Information

The HIPAA Privacy Rule gives patients the right to request and receive an accounting of all disclosures of their PHI made by the covered entity, with certain exceptions, for up to six years after the disclosure. The following disclosures of PHI are excluded from the accounting requirement: (1) to the patient, (2) for treatment, (3) for payment and health care operations, (4) for facility directories, (5) pursuant to authorization, (6) pursuant to a limited data set agreement, (7) to persons involved in the patient's care, (8) for correctional institutions, and (9) for certain law enforcement purposes. In addition, an accounting of disclosures log must be maintained in each patient's medical chart.

AVMHC management reported that they follow DMH Policy Number 500.6, *Accounting of Disclosures of Protected Health Information,* to track all non-routine disclosures. However, our review of four completed accounting of disclosures logs, which came from the above-mentioned ten medical charts, included only abbreviations or acronyms without an accompanying key or crosswalk. We requested AVMHC management to

define the abbreviations in the logs. Using those definitions, we subsequently determined that none of the logged disclosures were of the type required to be documented by the HIPAA Privacy Rule, as they met the exceptions of the accounting of disclosures of PHI requirement stated above.

These findings indicate that AVMHC workforce members do not have a clear understanding of the accounting of disclosures of PHI standard.

Recommendations

5. **Department of Mental Health Privacy Officer provide guidance to Antelope Valley Mental Health Center management on the Accounting of Disclosures of Protected Health Information standard, including ensuring that any abbreviations or acronyms used in the accounting of disclosures logs are clearly defined.**

6. **Antelope Valley Mental Health Center management ensure that workforce members are re-trained on the Department of Mental Health Policy Number 500.6, Accounting of Disclosures of Protected Health Information.**

Minimum Necessary Standard

When using, disclosing, or requesting PHI from another covered entity, the HIPAA Privacy Rule requires a covered entity to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. OCR provides covered entities with flexibility to address their unique circumstances, and make their own assessment of what PHI is necessary for a particular purpose.

Discussions with AVMHC management indicate that workforce members are aware of the minimum necessary standard.

HITECH Act Breach Notification Rule

HHS issued regulations requiring health care providers to notify patients when their health information is breached. Specifically, health care providers and other covered entities must promptly notify affected patients of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 patients. Breaches affecting fewer than 500 patients will be reported to the HHS Secretary annually. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate. Further, HHS' Breach Notification regulations emphasize the importance of ensuring that all workforce members are appropriately trained and knowledgeable about what constitutes a breach and on the

policies and procedures for reporting, analyzing, and documenting a possible breach of unsecured PHI.

AVMHC management informed us that the workforce members are aware that they must report all incidents involving suspected or actual breaches to their immediate supervisors, who will report to the DMH Privacy Officer. AVMHC did not report any breaches to the CHPO or OCR during Fiscal Year 2014-15. We reviewed DMH Policy Number 500.28, *Responding to Breach of Protected Health Information,* and noted that it provides clear guidance to workforce members in the event a breach or suspected breach of PHI is discovered.

Conclusion

We discussed our findings with DMH and AVMHC management on December 7, 2015. Overall, our review indicates while there were areas of noncompliance, DMH has initiated substantial efforts to comply with the HIPAA Privacy regulations, as indicated by their attached response. We will follow up with DMH management in 120 days from the date of this report to ensure all findings have been addressed. We thank DMH's Privacy Officer and AVMHC managers and staff for their cooperation and assistance during this review.

If you have any questions, please call me or your staff may contact Linda McBride, CHPO, at (213) 974-2166.

JN:AB:PH:RGC:LTM:JC

Attachment

c: Sachi A. Hamai, Chief Executive Officer
Mary C. Wickham, County Counsel
Stephanie Jo Reagan, Principal Deputy County Counsel
Judith Weigand, Compliance Officer, Department of Mental Health
Ginger Fong, Privacy Officer, Department of Mental Health
Audit Committee
Health Deputies

LAC DMH
LOS ANGELES COUNTY DEPARTMENT OF MENTAL HEALTH
550 S. VERMONT AVE., LOS ANGELES, CA 90020 HTTP://DMH.LACOUNTY.GOV

ROBIN KAY, Ph.D.
Acting Director
DENNIS MURATA, M.S.W.
Acting Chief Deputy Director
RODERICK SHANER, M.D.
Medical Director

Date: January 5, 2015

To: Linda McBride,
Chief HIPAA Privacy Officer

From: Ginger Fong
DMH Privacy Officer

This is our response to the Auditor-Controller's Draft report concerning compliance with the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) at Antelope Valley Mental Health Center (AVMHC).

Auditor- Controller Recommendation #1

Department of Mental Health Management establish and/or strengthen procedures to ensure that user accounts and access to information technology resources for transferred and/or terminated employees and contractors are disabled/removed timely. Procedures should clearly describe the process for communicating terminations and transfers to security administrators, and for monitoring, reviewing, and terminating access, as appropriate.

AVMHC Response:

AVMHC agrees with the Auditor-Controller's recommendation.

Procedures were updated to control access due to an employee's role or status change. Protocol has been established for employees who have been transferred and/ or terminated. Upon employee's transfer and/or termination date, AVMCH Local User Administrator (LUA) of AVATAR deactivates employee's access under the off boarding process, which deactivates the employee's access to AVATAR under AVMHC or AVWEC.

Outgoing Supervisor or Manager will notify the Information Security Division within CIOB immediately by submitting a Service Catalog request specifying the change (termination or suspension) in access that should be made and the effective date of the change. The notification must be made prior to the effective date of the change except in unanticipated or emergency events. The Incoming Supervisor or Manager will notify the ISD within CIOB immediately by submitting a Service Catalog request specifying the change in access that should be made appropriately to the user's role base.

Presently Human Resource Bureau's procedure is to send a list of terminations to CIOB to inform them of who has been terminated during the past week. These communications are done via email. However, there is a gap in the time that the notifications are not done in a timely manner for terminations and HRB and CIOB is aware that the requirements also apply to employee's who have transferred or have promoted. Currently HRB and CIOB are in discussion for ongoing efforts to implement steps to address the process as well as to monitor and review the procedures established in the updated procedures cited in Procedures No. 500.36.37 Procedures for Preventing Unauthorized Access (effective 12/21/15)

Auditor- Controller Recommendation #2

Antelope Valley Mental Health Center management ensure that the Wellness Center's medical records room is properly secured by restricting access to only those workforce members who have a business need, and assign a workforce member to log and track the removal and return of paper charts.

AVMHC Response:

AVMHC agrees with the Auditor-Controller's recommendation.

The access key pad code to the medical records room at AVWEC was changed as of 12/18/15 to limit staff access to the medical room. Staff access to the medical room consist of Wellness Center supervisor, front office staff, program manager II and staff assistant I. Protocol has been implemented to log and track the removal and return of all paper charts to include date and time of chart being checked out and returned.

Auditor- Controller Recommendation #3

Antelope Valley Mental Health Center management remind Wellness Center workforce members to take precautions to prevent unauthorized physical access to sensitive information, including storing protected health information in locked drawers or cabinets when unattended.

AVMHC Response:

AVMHC agrees with the Auditor-Controller's recommendation.

AVMHC and AVWEC have reviewed county policy on safeguarding consumer PHI and HIPAA Policies during all staff meeting on October 15, 2015. Further HIPAA training will be provided by Ginger Fong, HIPAA Privacy Officer for all staff in February 2016.

Auditor- Controller Recommendation #4

Antelope Valley Mental Health Center management ensure all workforce members, including locum employees, promptly receive the required HIPAA training, and maintain evidence documenting that training was completed.

AVMHC Response:

AVMHC agrees with the Auditor-Controller's recommendation.

Protocols are in place to ensure that all employees and volunteers are trained in Departmental HIPAA trainings upon start date with the DMH. All Locum employees at AVMHC have completed required HIPAA training as well as newly hired staff.

Auditor- Controller Recommendation #5

Department of Mental Health Privacy Officer provide guidance to Antelope Valley Mental Health Center management on the Accounting of Disclosures of Protected Health Information standard, including ensuring that any abbreviations or acronyms used in the accounting of disclosures logs are clearly defined.

AVMHC Response:

AVMHC agrees with the Auditor-Controller's recommendation.

Abbreviations or acronyms will no longer be utilized with the accounting of disclosures log. All employees have been instructed and protocol has been set to fully complete the accounting of disclosures of PHI in the log in detail. HIPAA Privacy Officer will provide training for all staff to review the requirements to complete the accounting of disclosure log.

Auditor- Controller Recommendation #6

Antelope Valley Mental Health Center management ensures that workforce members are re-trained on the Department of Mental Health Policy Number 500.6, Accounting of Disclosures of Protected Health Information.

AVMHC Response:

AVMHC agrees with the Auditor-Controller's recommendation.

All employees at AVMHC and AVWEC have been issued a copy of Department of Mental Health Policy Number 500.6. Further training will be provided by Ginger Fong, HIPAA Privacy Officer for all staff in February 2016.

Procedures for Preventing Unauthorized Access
Requirements to Control Access Due to a Subordinate's Role or Status Change

- **Procedures Number:** 500.36.37
- **Version Number:** 01
- **Effective Date:** 12/21/2015
- **Approved By:** Departmental Information Security Officer (DISO)
- **Date Approved:** 12/21/2015

- **Background:**

Healthcare organizations are required to protect electronic protected health information (EPHI), such as electronic health records, from internal and external risks. To mitigate these risks, a covered entity must implement technical safeguards as required by the HIPAA Security Rule and may use any security measures that allow it to reasonably and appropriately do so. In addition, a covered entity may incorporate industry best practices to enhance their overall security as needed.

The Security Rule defines technical safeguards in § 164.304 as "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

The Access Control standard requires a covered entity to: "Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)[Information Access Management]."

A covered entity can comply with this standard through a combination of access and technical controls. There are a variety of access and technical controls that are available within most information systems. The HIPAA Security Rule does not identify a specific type of access control method or technology to implement.

Regardless of the technology or information system used, access controls should be appropriate for the user's role and/or function, given on an "as need" basis, and the least amount of access given to perform their job function. Of equal importance to granting access, access modification or termination must take place as soon as the user's role changes or they leave the position that warranted system access initially. Any user title or role change, or transfer within DMH must trigger a review of the user's system access privileges. A user that leaves DMH must have their system access privileges terminated immediately. It is a matter of law.

Purpose:

These procedures identify the responsibilities that managers and supervisors must carry out in a timely manner in order to prevent unauthorized access to resources no longer needed by a user or no longer justified by the user's current role or duties.

❖ **Scope**

This procedure applies to all LACDMH employees that manage or supervise, employees, contractors, volunteers, interns, trainees, or any person who conducts work for LACDMH that involves authorized access to County computing resources. All such managed or supervised personnel must have appropriate authorizations for system access limited to the minimum required to perform their job functions. The managers and supervisors are responsible for reporting to the appropriate bureaus and units any title or role changes, inter-departmental transfers, and terminations as soon as they are aware of the change. Such report should occur prior to the effective date of a change or termination except in the case of an immediate and unexpected change of role or duties or immediate termination. In that case the reporting as soon as they are aware of the change or termination still applies, even if it is the same date the unanticipated event occurred.

❖ **Procedures**

It is MANDATORY that following procedures are followed by all LACDMH employees performing in a managerial or supervisory capacity when a change in role or employment status takes place for any person who conducts work for LACDMH and is under their authority:

- **Outgoing Supervisor or Manager:**

Notify the LACDMH Information Security Division within CIOB immediately by submitting a Service Catalog request specifying the change in access that should be made and the effective date of the change. The notification must be made prior to the effective date of the change except as described above for unanticipated or emergency events.

- **Incoming Supervisor or Manager:**

Notify the LACDMH Information Security Division within CIOB immediately by submitting a Service Catalog request specifying the change in access that should be made and the effective date of the change. The notification must be made prior to the effective date of the change except as described above for unanticipated or emergency events.

- **Information Security Division of CIOB:**

1. Will provide a copy of the notification to DMH Human Resources for confirmation purposes.
2. If there is doubt about the change in system access that should be made, the Information Security Division will contact the applicable manager for clarification.
3. Will notify others involved in system access such as ISD, CIOB Network Security, IBHIS System Administrator, IS System Administrator, and others as the case requires.
4. Communicate completion of the access changes to the applicable supervisor(s) or manager(s).

❖ **Contact:**

Chief Information Office Bureau/Information Security (213) 251-6466

Updated: December 2015